

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images,
Please do not report the images to the
Image Problem Mailbox.

JAPANESE UTILITY MODEL ABSTRACT (JP)

PUBLICATION

(51) IPC Code: H03K 3/84, H04K 1/10

(43) Publication No.: hei 3-120125

(43) Publication Date: 10 December 1991

(21) Application No.: hei 2-29466

(22) Application Date: 22 March 1990

(71) Applicant:

MITSUBISI Co., Ltd.

2-2-3, Marunouchi, Chiyodaku, Tokyo, Japan

(72) Inventor:

MINAKI MASAZUMI

(54) Title of the Invention:

Maximum long-period sequential generator

Object:

The present utility model relates to preventing unauthorized decoding of a maximum long-period sequential signal by a third person and improving the robustness of the maximum long-period sequential signal in secrecy communications.

What is claimed is:

In a maximum long-period sequential generator comprising a clock generator, n stages of flip-flops, where n is a positive integer, which are sequentially connected to one another and are commonly connected to a clock terminal of the clock generator to receive a clock signal, and a feedback logic circuit having an algorithm for generating a feedback signal to be fed back to the leading flip-flop through linear computations using the signals output from the n stages of flip-flops, the maximum long-period sequential generator further comprising a clock counter and switching a plurality of primitive polynomials in the feedback logic circuit whenever an output from the clock counter is received, to switch the feedback signal generating algorithm in response to the switching of the plurality of primitive polynomials.

公開実用平成 3—120125

⑬ 日本国特許庁(JP)

⑭ 実用新案出願公開

⑫ 公開実用新案公報(U) 平3—120125

⑮ Int. Cl. 5

識別記号

庁内整理番号

⑯ 公開 平成3年(1991)12月10日

H 03 K 3/84
H 04 K 1/00

A 8221—5J
Z 7117—5K

審査請求 未請求 請求項の数: 1 (全 頁)

⑰ 考案の名称 最大長周期系列発生器

⑱ 実 願 平2—29466

⑲ 出 願 平2(1990)3月22日

⑳ 考 案 者 三 奈 木 正 純 神奈川県鎌倉市上町屋325番地 三菱電機株式会社鎌倉製作所内

㉑ 出 願 人 三菱電機株式会社 東京都千代田区丸の内2丁目2番3号

㉒ 代 理 人 弁理士 大 岩 増 雄 外2名

明 細 書

1. 考案の名称

最大長周期系列発生器

2. 実用新案登録請求の範囲

クロック信号を発生するクロック発生回路と、初段以降はそれぞれ前段の出力が次段の入力に接続され、上記クロック発生回路のクロック信号を共通にクロック端子に接続された n 段(n は正整数)のフリップフロップと、上記 n 段のフリップフロップの各出力信号を入力され、これに線型演算を行うことにより初段のフリップフロップへ供給するフィードバック信号を生成するアルゴリズムを備えたフィードバック論理回路とを有する最大長周期系列発生器において、上記クロック信号を入力されてクロック数を計数するクロック計数回路を設け、上記クロック計数回路の計数出力を入力される度に上記フィードバック論理回路において複数の原始多項式を切り替え、これに応じてフィードバック信号の生成アルゴリズムを切り替えることを特徴とする最大長周期系列発生器。

3. 考案の詳細な説明

〔産業上の利用分野〕

この考案は、デジタル通信、計測等の分野でよく用いられる最大長周期系列発生器に関するものである。

〔従来技術〕

デジタル通信の分野においては、情報源から信号は一般に“1”及び“0”の2値からなる数値列に変換され、この2値により搬送信号を変調することによって行われる。

情報源からの信号としては、例えば音声や画像等があり、それぞれ特有の物理的な性質を有している。音声に係わる性質としては有音期間と無音期間が間欠的に現れ、また画像に係わる性質としては隣接する画素の相関が極めて高いことがあげられる。即ち、いずれの場合も、情報源の信号としては、ある一定期間は変化が全くないか、あるいは変化の小さい状態が続き、またある一定期間は有意な情報が続き、これらの状態が繰り返されることが多い。

通信において，上記のように情報源からの信号の変化が小さい状態は好ましくない影響を与えることが多い。例えば，情報源からの信号が変化する期間はこれによって変調される搬送信号は適度にスペクトラムが拡散されるが，情報源からの信号の変化が小さい場合は搬送波は帯域が広がらず，電力束密度が規定値を越え，通信系の障害となることが多い。情報源からの信号によらず“1”及び“0”の数値列の変化を保証するための手段として，一見不規則に変化するいわゆるランダム雑音状の信号により情報源からの信号を予め拡散し，これによって搬送信号を変調することが有効である。

このように，ランダム雑音状の信号は電力スペクトラムを拡散させる際に有用であるが，一方，雑音としての性質をより積極的に利用することも行われる。即ち，送信側で情報源からの信号とランダム雑音状の信号との排他的論理和をとり，受信側で再び受信信号と送信側で用いたものと同じランダム雑音状の信号との排他的論理和をとるこ

とによって、もとの情報源からの信号を再生することが出来る。この場合は、一見ランダムと見られる性質を積極的に利用して、いわゆる暗号化の手段として用いられる。送信側と受信側のみが知り得るランダム状の信号によって暗号化された情報は、ランダム状の信号の詳細な性質を知らない第3の傍受者がこれを解読することが困難であり情報の秘匿化に効果がある。

その他、通信、計測等の分野でランダム状の信号は広く用いられている。

以上にその用途の一端を紹介したランダム状の信号の代表的なものに最大長周期系列 (Maximum length shift register sequence) 符号があげられる。最大長周期系列符号は一般にM系列符号と呼ばれ、代表的な巡回符号として位置づけられるものである。

第2図に従来の最大長系列符号発生器の構成例を示す。

図において、(1)はクロック発生回路、(2)はクロック発生回路(1)から出力されるシフトクロック、

(4)

(3₁) ~ (3₃) はそれぞれ第 1 段, 第 2 段, 第 3 段のフリップフロップ, (4₁) ~ (4₃) はそれぞれ第 1 段, 第 2 段, 第 3 段のフリップフロップ (3₁) ~ (3₃) から出力されるシフト出力, (7) はシフト出力 (4₁) ~ (4₃) を分岐して入力され, 第 1 段のフリップフロップへの入力信号としてフィードバック信号を生成するフィードバック論理回路, (8) はフィードバック論理回路 (7) から出力されるフィードバック信号である。

フリップフロップ (3₁) ~ (3₃) は, それぞれ前段の出力が次段の入力に接続され, クロック発生回路 (1) のシフトクロック (2) をそれぞれのクロック端子に共通に入力され, これにより順次シフト動作を行う 3 段のシフトレジスタを構成している。

フィードバック論理回路 (7) は上記各フリップフロップ (3₁) ~ (3₃) のシフト出力 (4₁) ~ (4₃) を入力されて所要の演算を行い, フィードバック信号を生成する。ここで所要の演算とは最大長周期系列を生成するためのアルゴリズムに従った演算であり, この場合, 演算に用いる 3 次の原始多項式は

(5)

$X^3 + X^2 + 1$ または $X^3 + X + 1$ である。

上記のようにして 3 段のフリップフロップにより構成された最大長系列符号は、 $2^3 - 1 = 7$ ビットを 1 周期とする符号となる。一般に n 段のフリップフロップで構成した場合の符号長は $2^n - 1$ となることが知られている。

〔考案が解決しようとする課題〕

上記構成による最大長周期系列発生器において、出力信号のランダム性は符号長によりシフトレジスタの段数即ち使用するフリップフロップの個数に依存する。符号長は前記した通り段数を n 段とすれば $2^n - 1$ となるので、段数を増やすことによって出力信号のランダム性は指数関数的に増大する。

しかし、上記のようにして生成した最大長周期系列符号を、例えば秘匿通信に使用する場合は、周期を十分長くとる必要がある。無限長の符号系列を用いたいいわゆるバーナム暗号は第三者による解読を許さない優れた暗号であることが知られているが、その反面、有限長のものを用いた場合は、

符号自身の持つ線型性から第三者による解読が大きな困難なく可能であるという課題があった。

周期を長くするためにはフリップフロップの段数を増加する必要があり、回路規模の増大と、それに伴って電力、重量等の増加を招くことになる。

また、符号長を無限にすることは実現が不可能であり符号自身の持つ線型性に起因する上記課題を解決するのは不可能である。

この考案は最大長周期系列に係わる上記の課題を解決するためになされたものであり、最大長周期系列符号の第三者の解読を困難とすると共に秘匿通信における最大長周期系列符号の持つ脆弱性を改善することを目的とする。

〔課題を解決するための手段〕

この考案に係わる最大長周期系列発生器は、 n 段のシフトレジスタを駆動するシフトクロックを計数するクロック計数回路を設け、これにより周期を計ることによって一定周期ごとにフィードバック論理回路の設定を変更し、異なった原始多項式による系列を発生するようにしたものである。

〔作 用〕

この考察においては、一定周期ごとに異なった原始多項式による最大長周期系列を生成するため、それぞれ異なった符号系列の持つ符号を繋げることによって等価的に符号長を増加させるのみならず、最大長周期系列がよく知られていることに起因して、特に秘匿通信における最大長周期系列符号の持つ脆弱性を改善することが可能となる。

〔実施例〕

第1図はこの考察の一実施例を示す構成図である。

図において、(1)から(4)及び(7)、(8)は上記従来装置と全く同一のものである。また、(5)はシフトクロック(2)を入力されてクロックの個数をカウントするクロック計数回路、(6)はクロック計数回路(5)のクロック計数出力である。

シフトクロック(2)は、フリップフロップ(3₁)～(3₃)を駆動し、シフト動作を行うと同時にクロック計数回路(5)によってクロック数をカウントされる。クロック計数回路(5)はクロック数を予め設定

された数だけカウントすると，クロック計数出力(6)を生成する。フィードバック論理回路(7)はクロック計数出力(6)が入力される度に原始多項式を切り替え，これに応じた論理処理を行うことによってフィードバック信号(8)を生成する。

第1図の実施例では，フリップフロップ(3₁)～(3₅)は3段で構成されており，この場合，前述の通り原始多項式は $X^3 + X^2 + 1$ 及び $X^3 + X + 1$ の2種である。従って，フィードバック論理回路(7)には予めこれら2種の原始多項式に対応した論理動作をする論理回路を用意し，クロック計数出力(6)が入力される度にこれを一方から他方へ切り替えて異なった系列の符号を生成する。

〔考案の効果〕

以上のように，この考案によれば一定周期ごとに異なった原始多項式による最大長周期系列を生成するため，それぞれ異なった符号系列の持つ符号を繋げることによって，シフトレジスタの段数を増加することなく等価的に符号長を増加させることが可能となる。また，最大長周期系列はその

性質が広く知られており，秘匿通信に用いられる場合，その解読は比較的容易とされているが，予め送信側と受信側のみが知り得る周期を設定し，これによって原始多項式を切り替えて用いることにより第三者の解読が困難となり，最大長周期系列がよく知られていることに起因して，特に秘匿通信における最大長周期系列符号の持つ脆弱性を改善することが可能となる。

なお，実施例ではシフトレジスタの段数は3段であるが，任意の段数の最大長周期系列について実施可能であることは言うまでもない。

4. 図面の簡単な説明

第1図はこの考案の一実施例を示す装置の構成図，第2図は従来の装置を示す構成図である。

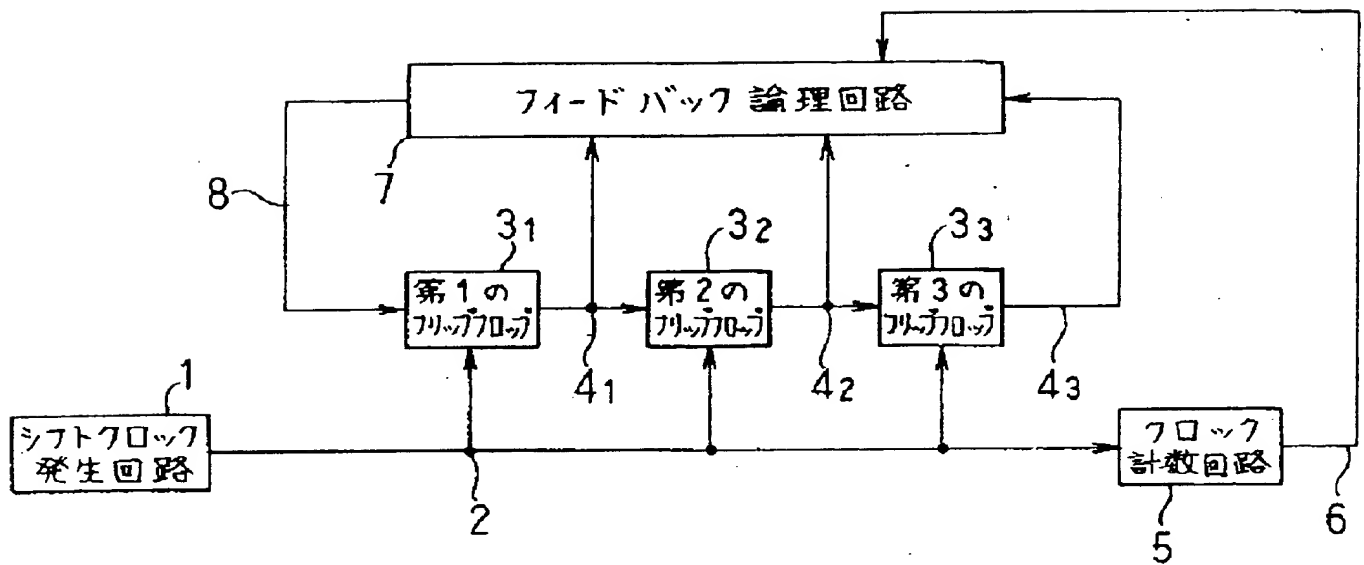
図において，(1)はシフトクロック発生器，(3₁)～(3₃)はフリップフロップ，(5)はクロック計数回路，(7)はフィードバック論理回路である。

図中，同一符号は同一または相当部分を示す。

代理人 大 岩 増 雄

(10)

第 1 図



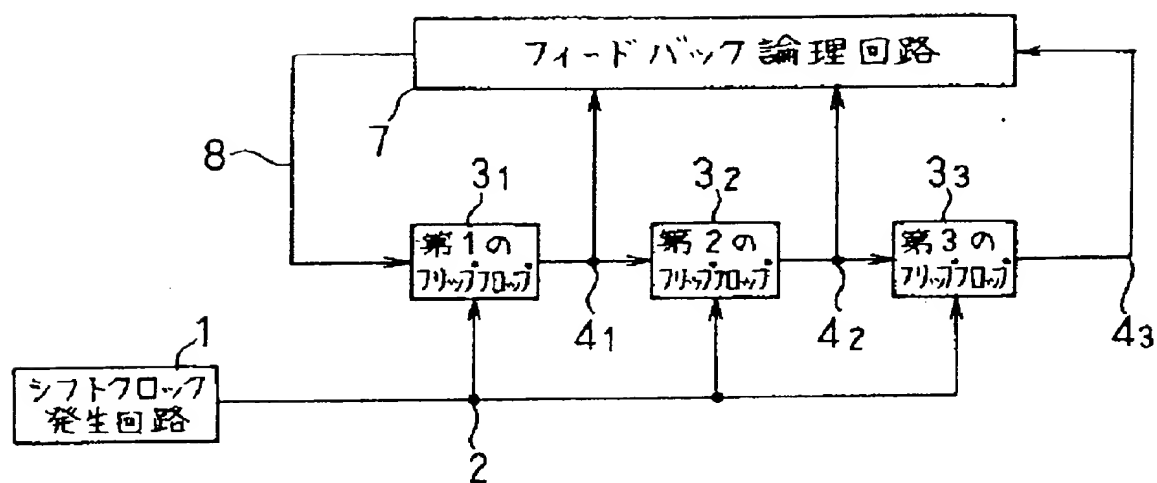
- 2 : シフトクロック
- 4 : シフト出力
- 6 : クロック計数出力
- 8 : フィードバック信号

実開3-120125

代理人 大 岩 増 雄

294

第 2 図



実開3-120125

代理人 大 岩 増 雄